7. Nikolenko T.M. Modelirovanie rasseyaniya parov szhizhennogo prirodnogo gaza v atmosfere. [Simulation of vapor dispersion of liquefied natural gas in the atmosphere]. *Tekhnosfernaya bezopasnost' kak kompleksnaya nauchnaya i obrazovatel'naya problema: materialy Vserossiiskoi konferentsii, Sankt-Peterburg, 4–6 oktyabrya 2018 g*. SPb.: Izd-vo Politekhn. un-ta, 2018; 251-256. (In Russian).

8. Safonov V.S. Ob osobennostyakh effekta bystrogo fazovogo perekhoda pri avariinykh razlivakh SPG na vodnoi poverkhnosti [On the features of the effect of rapid phase transition in emergency spills of LNG on the water surface]. *Nauchno-tekhnicheskii sbornik Vesti gazovoi nauki.* 2018; (4): 105-114. (In Russian).

9. Starovoitova E.V., Galeev A.D., Ponikarov S.I. Formirovanie vzryvoopasnogo oblaka pri avariinom vybrose szhizhennogo uglevodorodnogo gaza v atmosferu [Formation of an explosive cloud during an emergency release of liquefied petroleum gas into the atmosphere]. *Vestnik Kazan. Tekhnol. Un-ta.* 2012; (14): 213-214. (In Russian).

10. Shebeko A.Yu., Shebeko Yu.N., Gordienko D.M. Primenenie programmnogo kompleksa FDS 5 dlya raschetnoi otsenki parametrov rasseyaniya prolivov szhizhennogo prirodnogo gaza [Application of the FDS 5 software package for the calculated estimation of the parameters of dispersion of liquefied natural gas straits]. *Pozharnaya bezopasnost'.* 2013; (1): 34-38. (In Russian).

УДК 378.4

АНАЛИЗ ОПАСНОСТЕЙ ЦИФРОВИЗАЦИИ ОБЩЕСТВА

Попков А.В., к.пед.н., доцент кафедры безопасности жизнедеятельности, ФГБОУ ВО «Удмуртский государственный университет», г. Ижевск, Россия; ORCID: https://orcid.org/0000-0003-2979-6674; E-mail: safeman@inbox.ru

ANALYSIS OF SOCIETY DIGITALIZATION DANGERS

Popkov A.V., Candidate of Pedagogic Sciences, associate professor, Department of life safety, Udmurt state university, Izhevsk, Russia; ORCID: https://orcid.org/0000-0003-2979-6674; E-mail: safeman@inbox.ru

Получено 9.11.2020, после доработки 20.11.2020. Принято к публикации 3.12.2020.

Received 9.11.2020, after completion 20.11.2020. Accepted for publication 3.12.2020.

Попков, А. В. Анализ опасностей цифровизации общества / А. В. Попков // Вестник НЦБЖД. – 2021. – № 2 (48). – С. 105–111.

Popkov A.V. Analysis of society digitalization dangers. *Vestnik NTsBZhD.* 2021; (2): 105–111. (In Russ.)

Аннотация

Рассмотрены информационные технологии в аспекте актуальных и потенциальных опасностей в условиях цифровизации общества. Показаны предпосылки и факторы их возникновения. Выделены, обобщены и упорядочены их основные источники и негативные последствия.

Ключевые слова: информационные технологии, информационные риски и угрозы, информационное общество, кибербезопасность, защита информации, киберугроза, кибератака, утечка данных

Abstract

Information technologies are considered in the aspect of actual and potential dangers in

context of society digitalization. Preconditions and factors of their occurrence are shown. Their main sources and negative consequences are highlighted, summarized and ordered.

Keywords: information technology, information risks and threats, information society, cybersecurity, data protection, cyber threat, cyberattack, data leak

Развитие и совершенствование информационных технологий (далее – ИТ) привели к их проникновению практически во все сферы деятельности современного общества. Широкое использование электронных систем, компьютерной техники и средств телекоммуникаций уже привело к повсеместной автоматизации производственной сферы, созданию информационных инфраструктур не только локального, но и глобального характера. В настоящее время по своему социальному значению масштабы информатизации (цифровизации) общества сопоставимы с его индустриализацией. Можно сказать, что наступила эра информационного общества.

Заметим, что в настоящее время население нашей планеты составляет 7,7 млрд человек. Также в отчете Digital 2020 указано, что в 2019 г. среднестатистический пользователь проводил в Интернете 6:43 ч. в сутки, что составляет примерно 40% времени его бодрствования. Большую часть этих пользователей составляет молодежь.

Исследование, в котором приняли участие около 1000 студентов и школьников г. Ижевска, показало высокий уровень владения информационными технологиями и их частое использование для различных целей (рис. 1, 2).

Рис. 1. Частота контактов с разными видами информационных технологий

Биологическая среда обитания человека большей частью фактически заменена на технологическую. Виртуальная среда, в которой действует человек, не является естественной (природной) средой, а цифровое пространство, в котором он формируется, работает и взаимодействует, обладает значительно большим многообразием по сравнению с природным. И эта часть среды обитания человека постоянно расширяется. Цифровое общество, в котором скорость реализации многих процессов постоянно растет, предоставляет его членам новые возможности. В условиях, когда ключевое значение приобретают ИТ, направленные не столько на производство и распределение услуг и товаров, сколько на самого человека [1], его личность, – сам человек меняется, становится иным. Эти технологии, имея прогрессивный и социально направленный характер, тем не менее, имеют пределы своего применения.

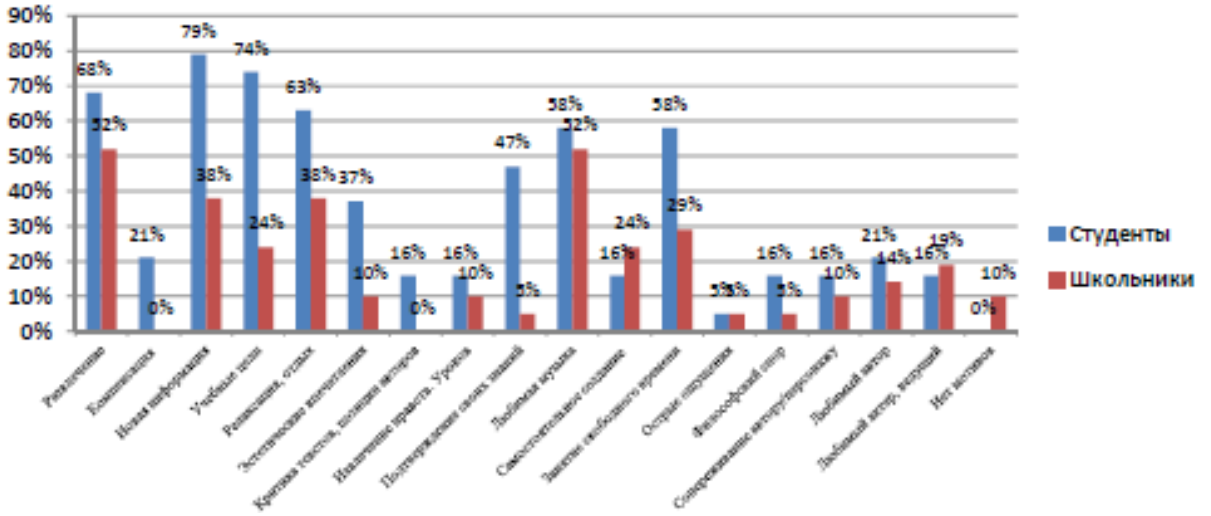

Рис. 2. Мотивы контактов и результаты восприятия (перцепции) ИТ у школьников и студентов

Переход через эти пределы может вызвать значительный ущерб как для отдельного человека, так и общества в целом.

В частности, уже сейчас мы наблюдаем целый ряд проблем, связанных с информационными рисками и угрозами личности [1, 4, 6]. Эти проблемы вызывают последствия, степень которых, на наш взгляд, еще до конца не оценена и не исследована.

Перейдем к рассмотрению обозначенных выше проблем. Каковы их причины и последствия? Сосредоточимся на тех основных информационных рисках и угрозах, которым подвержены члены цифрового общества.

Влияние на личность (интернет-аддикции)

Термин «интернет-аддикция» ввела психолог Кимберли Янг. В 1994 г. она разослала по сети анкеты и соотнесла ответы с общепринятыми критериями зависимости от химических веществ. Оказалось, заболеть Интернетом можно очень быстро – за полгода-год. Основными видами интернет-аддикций являются: изучение программ и функций компьютера – в ущерб остальной деятельности, навязчивая навигация по сайтам, компульсивные интернет-покупки, чрезмерная увлеченность компьютерными и онлайн-играми, зависимость от общения в чатах и форумах, чрезмерная увлеченность социальными сетями с навязчивой перепроверкой лайков и постов людей и др.

Под влиянием интернет-аддикций сужается спектр увлечений, теряется интерес к монотонной деятельности, возникают отвлеченность внимания и нарушения концентрации, искажаются семейные отношения. Это увеличивает раздражительность и усталость. При лишении доступа к сети и сетевым устройствам настроение падает до «тоскливо-злобного». В некоторых случаях проблема бывает настолько серьезной, что возникают суицидальные высказывания и угрозы.

Возможность отслеживания

Массовая «смартфонизация», повсеместно установленные камеры внешнего наблюдения позволяют определить местоположение, а в ряде случаев и личность наблюдаемого. Интернет-браузеры, установленные на персональных компьютерах пользователей, запоминают частоту и тематику их поисковых запросов. Это позволяет подбрасывать им соответствующие рекламные ссылки и сетевые электронные ресурсы, оказывающие на них определенное информационное воздействие, далеко не всегда позитивного характера. Велика вероятность, что даже простое посещение

вредоносного веб-сайта и просмотр его страницы и/или рекламного баннера приводят к теневой загрузке нежелательных, вредоносных файлов.

Миллионы пользователей социальных сетей и сайтов знакомств добровольно публично «обнажаются», сообщая о себе буквально всю информацию: о финансовом положении, интересах и предпочтениях, политических взглядах, семейной жизни, друзьях, эмоциях. При этом значительная доля этих пользователей имеет сотни «друзей», с которыми они не только обмениваются сообщениями, но и предоставляют им доступ к личной странице, даже будучи знакомы лишь с их цифровым профилем.

Использование личных данных

Все вышеперечисленные реалии цифрового общества создают возможности не только для отъема личных данных у его членов, но и для их обработки и концентрации в базах данных, что и происходит. Достаточно привести лишь один пример. Один из крупнейших дата-брокеров в США компания Acxiom Corp., еще по оценкам 2017 г. владела персональной информацией, охватывающей примерно 80% взрослого населения США и полмиллиарда человек за их пределами [2]. Эта информация дифференцируется по так называемым профайлам, которые по сути являются личными анкетами, содержащими до 50 параметров «цифровой» личности: от девичьей фамилии матери до перечня мелких административных правонарушений. С целью получения прибыли Acxiom Corp. и другие дата-брокеры (например: Oracle, Intelius, Rapleaf) продают оптом (в виде структурированных информационных массивов, сведенных в базы данных) профайлы третьим лицам. Например, таким гигантам как Google, Microsoft, Facebook, а также многим кредитным организациям. В обладании такой информацией заинтересованы не только официально действующие организации, но и различного рода преступные группы, теневые структуры, террористические, экстремистские организации и киберпреступники.

Несовершенство технических систем защиты информации

Проблемы, связанные с нарушением информационной безопасности, приобрели уже такой массовый характер, что вышли за пределы интересов не только отдельных организаций и личностей, но и государств, и тем самым имеют стратегическое значение. Об их масштабах мы можем судить по данным в СМИ, различного рода публикациям [3], которые в полной мере не отражают реальной ситуации. Но даже этого достаточно для понимания того, что вопросы кибербезопасности носят глобальный характер. Обеспечение кибербезопасности является одним из приоритетных направлений нейтрализации информационных угроз через реализацию соответствующих мероприятий на всех уровнях, в том числе на государственном [4] и международном.

Ситуация, когда сам пользователь инициирует такие последствия, отчасти вызвана его недостаточной обученностью в области кибербезопасности. Если говорить о России, то основные причины этого – фрагментарность обучения основам кибербезопасности на всех уровнях образования [5], отсутствие системного подхода, отдельных учебных программ и предметных областей, направленных на повышение компетентности обучающихся в области информационной безопасности. К решению этих проблем подталкивает и тотальный дефицит квалифицированных кадров в области кибербезопасности.

Таким образом, под угрозой находятся практически все информационные ресурсы: мобильные устройства граждан и их ПК, работающие в Интернете, социальные сети, веб-сайты и базы данных различных организаций (в том числе крупных коммерческих, государственных и промышленных компаний), предприятия инфраструктуры и здравоохранения, сети банков, системы онлайн-банкинга, интернет-магазины, он-

лайн-сервисы по продаже услуг и др. При этом в зоне повышенного риска находятся бизнес и инфраструктурные объекты.

Основные источники угроз для информационной безопасности граждан, социальных групп, компаний, государств и их последствия приведены в табл. 1.

Таблица 1

Источники киберугроз	Риски
Социальные сети в целом, форумы, чаты, мессенджеры	Потеря личных данных, интернет-аддикции, кибербуллинг, другие негативные воздействия психоэмоционального характера.
Сетевые сообщества девиантной направленности (террористические, националистические и экстремистские группы и сайты, религиозные секты и др.)	Противоправные деяния: кибертерроризм, компьютерная педофилия, диффамация и др. Угрозы жизни и здоровью членов. Потеря финансовых средств и имущества. Вербовка в преступные организации.
Деструктивные группировки в социальных сетях («Беги или умри», «Группы смерти» [4] и др.)	Угрозы жизни и здоровью членов групп.
Вредоносные сайты	Заражение ПК вредоносными программами различных типов и назначений, шпионскими программами типа Spyware / Malware, дестабилизация работы программного обеспечения.
Сбой систем информационной безопасности, их несовершенство. Умышленная утечка закрытой информации	Взлом баз данных инсайдеров, потеря личных данных и/или финансовых средств организаций, частных лиц, промышленный шпионаж и др.
Использование нелицензионного (пиратского) и непропатченного ПО	Повышение уязвимости ПК, взлом ПК.
Легальное ПО, содержащее скрытый функционал. Нелегальное ПО, не имеющее сертификат безопасности	Потеря личных и других данных, заражение вирусами, отказ ПК, кибершпионаж, вредоносные кибероперации.
Сайты-знакомств и интимных услуг, экстремальные порносайты	Потеря личных данных, шантаж, вымогательство, угрозы здоровью, рост половых преступлений.
Фишинговые сайты (сайты-двойники)	Потеря личных данных и/или финансовых средств, недостоверная или вредоносная реклама.
Фальшивые сайты-файлообменники, службы доставки	Потеря финансовых средств, моральный ущерб.
Онлайн-игры	Потеря финансовых средств, потеря личных данных, негативное информационно- психологическое воздействие, асоциальное поведение, игровая зависимость.
Ботнеты различных типов	Вымогательство, шантаж, потеря, уничтожение или зашифровка данных, частичная или полная потеря управляемости ПК и все последствия этого.

Окончание таблицы 1

Кибератаки (DDoS-атаки, Вайпер-атаки, MITM-атаки, APT-атаки2, атаки с помощью снифферов3 и др.)	Финансовый ущерб компаний и частных лиц, захват и уничтожение данных, деструктивное воздействие на инфраструктуры организаций и объектов и/или вывод их из строя, несанкционированное прослушивание каналов связи, дезинформация, кража интеллектуальной собственности и др. Национальная безопасность.
Различные варианты SMS- и GSM-фрода (телефонное мошенничество)	Потеря личных данных и финансовых средств.
Несанкционированная манипуляция данными и цифровой информацией из систем и сетей	Воздействия идеологического и информационно-психологического характера, продвижение политических позиций. Безопасность индивидуального, группового и массового сознания граждан. Национальная безопасность.

Таким образом, внедрение информационных технологий породило цифровой мир, в который так или иначе вовлечена большая часть общества. Этот мир трансформирует его жизнь и деятельность, во многом определяет его образ жизни, вызывает необходимость совмещать реальность и виртуальность.

В результате такой трансформации возникают новые информационные опасности как для общества в целом, так и для отдельно взятых социальных слоев, особенно молодежи. Отмечается тенденция роста их числа и уровня. В такой ситуации не стоит полагаться на процессы самоорганизации и саморегуляции общества. Здесь необходимы системные, фундаментальные исследования, направленные на выявление факторов, порождающих эти риски и угрозы, выработку механизмов их нейтрализации. Необходимо устранить запаздывание в развитии и совершенствовании систем защиты информации от систем их преодоления.

Список литературы

1. Катасонов, В. Бизнес-разведка : Что выуживает Facebook у своих клиентов / В. Катасонов // Свободная Пресса. – URL : https://svpressa. ru/economy/article/188785/ (дата обращения: 30.09.2020). – Текст: электронный.

2. Кибербезопасность 2019-2020 : тенденции и прогнозы // Positive Technologies. – URL: https://www.ptsecurity.com/upload/corporate/ru-ru/ analytics/cybersecurity-2019-2020-rus.pdf (дата обращения: 02.06.2020). – Текст: электронный.

3. Пази, М. Большой информационный взрыв. Объемы интернет-контента стремительно меняют инфосферу Земли / М. Пази // Русский репортер. – 2017. – № 2 (419). – С. 52–53.

4. Троицкая, О. Н. Подготовка будущих учителей математики и информатики к обучению школьников основам кибербезопасности / О. Н. Троицкая, Е. Д. Вохтомина // Информатика и образование. – 2019. – № 28. – С. 24–31.

5. Шваб, К. Четвертая промышленная революция / К. Шваб. – Москва : ЕКСМО, 2017. – 230 с.

6. Шпионские программы // Malwarebytes. – URL: https:// ru.malwarebytes.com/ spyware/ (дата обращения: 29.05.2020). – Текст: электронный.

References

1. Katasonov V. Biznes-razvedka: Chto vyuzhivaet Facebook u svoikh klientov [Business intelligence: What Facebook is fishing out from its customers]. *Svobodnaya Pressa*. URL: https://svpressa. ru/economy/article/188785/ (accessed: 30.09.2020). (In Russian).

2. Kiberbezopasnost' 2019-2020: tendentsii i prognozy [Cybersecurity 2019-2020: trends and forecasts]. *Positive Technologies.* URL: https://www.ptsecurity.com/upload/corporate/ru-ru/ analytics/cybersecurity-2019-2020-rus.pdf (accessed: 02.06.2020). (In Russian).

3. Pazi M. Bol'shoi informatsionnyi vzryv. Ob"emy internet-kontenta stremitel'no menyayut infosferu Zemli [Big information explosion. The volume of Internet content is rapidly changing the Earth's infosphere]. *Russkii reporter.* 2017; 2 (419): 52-53. (In Russian).

4. Troitskaya O.N., Vokhtomina E.D. Podgotovka budushchikh uchitelei matematiki i informatiki k obucheniyu shkol'nikov osnovam kiberbezopasnosti [Preparing future teachers of mathematics and computer science to teach students the basics of cybersecurity]. *Informatika i obrazovanie.* 2019; (28): 24-31. (In Russian).

5. Shvab K. Chetvertaya promyshlennaya revolyutsiya [The Fourth Industrial Revolution]. M.: EKSMO, 2017. 230 p. (In Russian).

6. Shpionskie programmy [Spyware]. *Malwarebytes.* URL: https:// ru.malwarebytes.com/ spyware/ (accessed: 29.05.2020). (In Russian).

УДК 614.8

ЦИФРОВОЙ ДВОЙНИК СИСТЕМЫ ПОЖАРНОЙ БЕЗОПАСНОСТИ НА ОСНОВЕ МОДЕЛИРОВАНИЯ ЕЁ МОЩНОСТИ КАК СЛОЖНОЙ СИСТЕМЫ

Сиразетдинов Р.Т., д.т.н., профессор кафедры динамики процессов и управления;
E-mail: rif-kat@inbox.ru;
Афанасьев В.М., доцент кафедры промышленной и экологической безопасности;
E-mail: abm5491@mail.ru;
Бжания А.Т., ассистент кафедры промышленной и экологической безопасности ФГБОУ ВО «Казанский национальный исследовательский технический университет им. А.Н. Туполева – КАИ», г. Казань, Россия;
E-mail: alina-hismatova@mail.ru

Получено 19.11.2020,
после доработки 30.12.2020.
Принято к публикации 25.01.2021.

DIGITAL TWIN OF FIRE SAFETY SYSTEM BASED ON MODELING ITS POWER AS A COMPLEX SYSTEM

Sirazetdinov R.T., Doctor of Engineering Sciences, Professor of the Department of process dynamics and management;
E-mail: rif-kat@inbox.ru;
Afanasiev V.M., Associate Professor at the Department of industrial and environmental safety;
E-mail: abm5491@mail.ru;
Bzhania A.T., assistant at the Department of industrial and environmental safety, Kazan research technical University named after A. N. Tupolev-KAI, Kazan, Russia;
E-mail: alina-hismatova@mail.ru

Received 19.11.2020,
after completion 30.12.2020.
Accepted for publication 25.01.2021.

Сиразетдинов, Р. Т. Цифровой двойник системы пожарной безопасности на основе моделирования её мощности как сложной системы / Р. Т. Сиразетдинов, В. М. Афанасьев, А. Т. Бжания // Вестник НЦБЖД. – 2021. – № 2 (48). – С. 111–117.

Sirazetdinov R.T., Afanasiev V.M., Bzhania A.T. Digital twin of fire safety system based on modeling its power as a complex system. *Vestnik NTsBZhD.* 2021; (2):111-117. (In Russ.)